Vanessa R. Waldref
United States Attorney
Eastern District of Washington
Richard R. Barker
Patrick J. Cashman
Assistant United States Attorneys
Post Office Box 1494
Spokane, WA 99210-1494
Telephone: (509) 353-2767

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA, Plaintiff, v. RONALD CRAIG ILG (a/k/a "SCAR215"), Defendant.	Case No. 2:21-CR-00049-WFN-1 United States' Response to Defendant's Motion to Exclude Dark Web Messages and Websites

The United States of America, by and through United States Attorney Vanessa R. Waldref and Assistant United States Attorneys Richard R. Barker and Patrick J. Cashman, respectfully submit this opposition to Defendant's motion to exclude Defendant's communications in which he solicited several dark web hitmen to assault a co-worker and his estranged wife. ECF No. 119.

INTRODUCTION

As set forth herein, the communications at issue are statements of a party opponent, admissible pursuant to Federal Rule of Evidence 801(d)(2)(A). At trial, the United States will elicit evidence from witnesses who obtained the messages directly from the dark

web. These witnesses will be able to authenticate the messages as true and correct copies of material obtained directly from the server where Defendant's messages were stored.

Defendant's reliance on *United States v. Vayner*, 769 F.3d 125 (2nd Cir. 2014) is misplaced. In *Vayner*, the Second Circuit emphasized that "'distinctive characteristics' of a document can sometimes alone provide circumstantial evidence sufficient for authentication" – e.g., attribution of a writing to a specific author "may be authenticated by evidence 'that the contents of the writing were not a matter of common knowledge.'" *Id.* at 133. As set forth in detail below, this is exactly what the government will do here. The Government will show Defendant is the author of these messages through Defendant's admitted use of moniker "Scar215," screenshots from his smartphone, and information, including the username and password for the dark web sites, located in a biometric safe possessed by Defendant at his residence. *See* Ex. A (Annotated copy of dark web messages reflecting corroboration that Defendant authored the messages) (filed under seal).

BACKGROUND

This case stems from Defendant's solicitation of various hitmen to assault a former co-worker (Victim 1) and kidnap Defendant's estranged wife (Victim 2). In March and April 2021, Defendant paid approximately $60,000 in Bitcoin to pay the purported hitmen. The FBI was alerted to Defendant's activities and ultimately recovered the actual messages and transaction records demonstrating Defendant's illicit conduct. Based on this evidence, the grand jury returned a superseding indictment on February 1, 2021 charging Defendant with seven counts related to Defendant's messages targeting Victims 1 and 2.

The dark messages in this case can be divided into two categories: *First*, the FBI obtained a transcript of Scar215's messages from the British Broadcasting Company and its partner "We're Novel." The transcript contains verbatim copies of Defendant's

messages. *Second*, the FBI obtained screenshots and video of the messages directly from the dark web sites. These were obtained pursuant to the execution of a number of search warrants pursuant to Rule 41(b)(6). The FBI accessed these messages directly from the dark web server using login credentials located inside Defendant's biometric safe. Various sources of information, discussed in detail below, and reflected in Exhibit A, demonstrate Defendant authored these messages. Notably, each of the messages the FBI obtained pursuant to Rule 41(b)(6) search warrants also were provided by the BBC – providing strong corroboration that the messages provided by the BBC are authentic. A small number of the messages obtained by the BBC were no longer available when the FBI accessed the dark websites via search warrant.

DISCUSSION

Defendant's motion appears to raise three arguments: (1) admitting the dark web messages would violate the confrontation clause; (2) the messages cannot be authenticated; and (3) the responses by the operators and administrators of the dark web sites are hearsay. ECF No. 119. Each of these arguments lacks merit.

1. Defendant's Messages on the Dark Web are Not Testimonial.

Defendant cannot hide behind the confrontation clause to shield his dark web messages from the jury. *See* ECF No. 9-14. The Confrontation Clause prohibits the "admission of testimonial statements of a witness who did not appear at trial unless he was unavailable to testify, and the defendant had had a prior opportunity for cross-examination." *Crawford v. Washington*, 541 U.S. 36, 53–54 (2004). This right applies only to testimonial evidence. *See Giles v. California*, 554 U.S. 353, 376 (2008). Testimonial evidence includes "formal statements to government officers, or formalized testimonial materials such as affidavits, depositions, and the like, that are destined to be used in judicial proceedings." *United States v. Brown*, 822 F.3d 966, 974 (7th Cir. 2016). Business records, however, are generally nontestimonial because "they are not made for

the purpose of later prosecution." *Id. Cf. Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 321 (2009) (noting that documents created for use at trial do not qualify as business records).

The dark web messages at issue in this case are not testimonial. Defendant sent the messages for purposes of soliciting a dark web hitman – not for use in some anticipated trial. Indeed, Defendant believed these messages would never see the light of day. Unfortunately, for him, he was wrong.

While Defendant contends that the copies of the messages provided to the FBI by the BBC are testimonial because those messages were captured by a source associated with the BBC, this does not somehow make the messages themselves testimonial. Again, Defendant was engaged in chats with administrators of the dark websites about having his estranged wife kidnapped and a former work colleague kidnapped. None of these communications were to law enforcement, and neither Defendant nor the dark web administrators created these messages in anticipation of litigation.[1]

[1] To the extent Defendant argues that the process by which the messages were obtained is somehow testimonial, the United States will call witnesses, including Special Agent Christian Parker, to describe how he accessed the dark web sites and recovered the messages at issue. *See* ECF No. 119. Specifically, the evidence at trial is anticipated to be that Special Agent Parker was able to access the sites associated with the dark web messages. Relying on a search warrant, Special Agent Parker used the log-in credentials found inside Defendant's safe to take screenshots and video of Defendant's messages on the dark web. Special Agent Parker obtained the messages directly from the websites Defendant used to solicit the dark web hitmen.

To be sure, certain dark web messages originally obtained by the BBC were no longer available when Special Agent Parker accessed the dark web sites. To the extent the United States seeks to introduce messages that were not recovered by Special Agent Parker, the United States anticipates that another witness – e.g., a records custodian will certify and/or testify that these messages are verbatim

2. Defendant's Dark Web Messages Are Admissible as Statements against a Party Opponent and Are Easily Authenticated.

Defendant's primary argument is that the United States cannot authenticate his messages from the dark web. ECF No. 119. Here the issue turns on whether there is sufficient evidence that Defendant sent and received the messages at issue.

a. Legal Standard

When online messages or communications are offered as evidence, Courts must determine whether the document itself is genuine: "To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a); *see also United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (requiring "a prima facie showing" that "a reasonable juror could find in favor of authenticity").

As an initial step, proof of authentication can be done through testimony or a records certification by a person "with knowledge" that the matter is what it is claimed to be." *United States v. Vayner*, 769 F.3d 125, 130 (2d Cir. 2014). For instance, a record custodian or a witness who viewed and recorded material on the website may testify that the record is in fact the same as what appeared on the site. *See id.* When doing so, "[t]he proponent need not rule out all possibilities inconsistent with authenticity, or . . . prove beyond any doubt that the evidence is what it purports to be." Rather, there must be "sufficient proof . . . so that a reasonable juror could find in favor of authenticity." *United States v. Vayner*, 769 F.3d 125, 130 (2d Cir. 2014) (internal quotation marks omitted).[2]

---

copies of messages obtained directly from the dark web servers, retained in the ordinary course, and thereafter provided to the government.

[2] Defendant's motion appears to argue that viewing a website and capturing screenshots from that site is insufficient to authenticate electronic evidence. ECF No. 119 at 2 (citing *Vayner*, 769 F.3d at 131). This is an incorrect statement of the law. In *Vayner*, the agent who viewed the website properly authenticated the existence and content of the website. *See* 769 F.3d at 131. The problem was that the

Where, as here, the government seeks to introduce the online communication as an admission of a party opponent, the government must provide sufficient evidence – whether direct or circumstantial – that the defendant authored the communication. *See, e.g.*, *Tank*, 200 F.3d 627 at 630 (requiring "a connection between the proffered evidence and the defendant."). Courts have made clear that "the Government may authenticate" online messages "with circumstantial evidence linking the defendant" to those messages. *See, e.g.*, *United States v. Lamm*, 5 F.4th 942, 948 (8th Cir. 2021). As one court put it: "To authenticate [online] records and messages, the government need[] only to 'produce evidence sufficient to support a finding' that the account belonged to [the defendant] and the linked messages were actually sent and received by him." *United States v. Barber*, 937 F.3d 965, 970 (7th Cir. 2019).

"The bar for authentication of evidence is not particularly high." *United States v. Isabella*, 918 F.3d 816, 844 (10th Cir. 2019); *see also United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007). In *Barber*, for example, the court reasoned that the evidence was sufficient to connect the account to the defendant because the account was "linked to his girlfriend's" and "linked to his cell phone." 937 F.3d at 970. A witness in the case also testified that he communicated with the defendant through the account. *Id.* The Court

---

government never offered sufficient evidence that the defendant authored the messages contained on the site. *See id.* In this regard, the Second Circuit explained:

> [A]ll the information contained on the [web] page allegedly tying the page to Zhyltsou was also known by Timku and likely others, some of whom may have had reasons to create a profile page falsely attributed to the defendant. Other than the page itself, moreover, no evidence in the record suggested that Zhyltsou even had a VK profile page, much less that the page in question was that page. Nor was there any evidence that identity verification is necessary to create such a page with VK, which might also have helped render more than speculative the conclusion that the page in question belonged to Zhyltsou.

769 F.3d at 132–33 (2d Cir. 2014) Unlike in *Vayner*, there is abundant evidence in this case that Defendant authored the communications in which he solicited a hitman to harm Victims 1 and 2.

explained that "[t]his was more than enough for a reasonable jury to conclude that the account belonged to Barber." *Id.*; *see also United States v. Lewisbey*, 843 F.3d 653, 658 (7th Cir. 2016) (relying on evidence such as the presence of a nickname, date of birth, address, email address, and photos on someone's Facebook page as circumstantial evidence that a page might belong to that person). Similarly, in *United States v. Browne*, the Third Circuit relied on circumstantial evidence that the suspect sent the social media messages at issue – including testimony that witnesses met with the suspect shortly after setting up meetings via the same social media account. 834 F.3d 403, 415 (3d Cir. 2016). Rejecting a challenge to the admissibility of the defendant's social media chats, the Third Circuit explained, the "authentication challenge collapses under the veritable mount of evidence linking" the Defendant with the incriminating chats. *Id.*; *see also United States v. Barnes*, 803 F.3d 209, 217 (5th Cir. 2015) (accepting admission of Facebook messages where a witness testified that she saw the defendant using Facebook, recognized his account, as well as his style of communicating).

Once the relatively low bar of admissibility is met, the defendant may "challenge the reliability of the evidence," e.g., "to minimize its importance, or to argue alternative interpretations of its meaning." *See Vayner*, 769 F.3d at 131. "[T]hese and similar other challenges," however, "go to the weight of the evidence – not to its admissibility." *Id.*

b. <u>Analysis</u>

Turning to the evidence[3] in this case, Defendant's "authentication challenge collapses under the veritable mount of evidence linking" the Defendant with the

[3] To the extent Defendant contends that the government cannot authenticate the very existence or content of the messages, he is wrong. Here, the FBI captured screenshots and video of the messages directly from the servers containing the dark web messages. The BBC likewise provided the government with verbatim copies of the messages at issue. *See* Ex. A. At trial, the FBI will attest that the screenshots and video are true and correct copies from the dark web servers. This is more than sufficient "for a

incriminating dark web chats. *See* 834 F.3d at 415. Here, Defendant admitted that he was hiring hitmen on the dark web using the moniker "Scar215." ECF No. 122-1 at 39. Among other things, he also admitted transmitting $10,000s of dollars in Bitcoin, consistent with the content of the dark messages. *Id.* at 33. Similarly, Defendant's messages – i.e., using the dark web moniker Scar215 to solicit hitmen to harm Victims 1 and 2 – are likewise admissions. *See* Fed. R. Evid. 801(d)(2)(A).

If this were not enough, Defendant's identity as the author of the dark web messages is corroborated by the content of the messages themselves. Notably, the messages contain unique identification and/or verification codes that Defendant saved to his phone and/or wrote down in a book, placed in his biometric safe, and sent to an encrypted email account. *See* Ex. A at 4. It is not a mere coincidence that these unique verification codes that appear in the dark messages were recovered from Defendant's safe and his phone. In addition, consistent with the plot to have Victim 2 kidnapped, Defendant's mistress confirmed that Defendant told her that he had paid hitmen on the dark web to harm Victim 2. *See* Bates 00000144.02.02.

Furthermore, the author of the dark messages also had access to intimate information that few, if anyone other than Defendant, possessed – e.g., divorce proceedings, motive to harm Victims 1 and 2, scheduling, and Bitcoin addresses. For example, Scar215 knew Victim 2's work schedule as well as the temporary visitation schedule for Defendant and Victim 2's minor child. *See* Ex. A at 17. Scar215 also knew information about Victim 2's family – about her older son and dog, which were to be used as leverage to get Victim 2 to return to Defendant and be intimate with him. *See id.*

---

reasonable jury could find in favor of authenticity." *Vayner*, 769 F.3d 125, 130; *see also United States v. Needham*, 852 F.3d 830, 836 (8th Cir. 2017) (holding that "[e]xibits depicting online content may be authenticated by a person's testimony that he is familiar with the online content and that the exhibits are in the same format as the online content.").

at 19. Tellingly, Scar215's messages demonstrate an urgency consistent with the schedule for Defendant's divorce proceedings. According to the messages, Defendant wanted the kidnapping completed prior to April 18, 2021. *Id.* at 14. The divorce proceedings were scheduled for April 19, 2021. Finally, the name "Scar215" and password, "Mufasa$$" are consistent with Defendant's affinity for lions, which witnesses described. *See* Ex. A at 5.

Defendant's Bitcoin transactions further corroborate that he is "Scar215" and paid approximately $60,000 in Bitcoin to have Victim 2 kidnapped. As set forth in detail in Exhibit A, Defendant conducted nearly all of his transactions on the dark web through one specific wallet – his "seed phrase wallet." Ex. A at 45. Defendant funded this wallet with money in his Coinbase account. *Id.* He also made direct deposits to the "seed phrase wallet" from ATMs in Spokane, Washington. *See id.* at 45. Defendant was even captured on camera making these the ATM deposits, which went directly into the seed phrase wallet and then on to the purported hitmen. *See id.* at 45. This is significant because the unique 12-word recovery code for the seed phrase wallet was found inside Ilg's biometric safe.[4]

Finally, when Defendant was caught, he took several actions demonstrating his consciousness of guilt. In fact, the same day the FBI confronted Defendant about his activities on the dark web, Defendant attempted to take his life – describing his

[4] Defendant's authorship of the dark web messages pertaining to Victim 1 is also compelling. The Bitcoin transaction records reflect that Defendant used same wallet to pay for the hits on *both* Victims. Again, there are photographs of Defendant uploading money to this unique cryptocurrency wallet – strong evidence of Defendant's identity as the author of the messages as Defendant controlled the wallet linked to the illicit payments. Similarly, the login credentials relating to the hit on Victim 2 – found in Defendant's safe – are the same as the moniker relating to Victim 1. Moreover, as is well documented in this case, Defendant had a motive for assaulting Victim 1. *See* ECF No. 106 at 9-10.

behavior/actions as an "irreparable fuck up." ECF No. 123 at 3-4. In a note to his family, Defendant prayed for forgiveness. *Id.* While in custody, Defendant attempted to tamper with one of the witnesses against him – begging the witness to marry him so he could have control over whether she would testify. *See* ECF No. 89 at 8-9. If she did so, Defendant offered to pay tuition for her children to attend private school in Spokane. *Id.* Defendant even directed the witness to burn evidence of his efforts to tamper with the witness. *Id.*

In short, there is ample evidence Defendant is the author of the dark web messages. While Defendant apparently will claim that someone else is responsible for those messages, there is no evidence corroborating his claims. Even if there were, the issue of whether Defendant is the author of these messages is one for the jury. The United States has more than sufficient evidence to meet the relatively low bar for authenticity and present the messages to the jury as a statement of a party opponent. *See Vayner*, 769 F.3d at 131 (once the relatively low bar of authenticity is met, challenges to authenticity "go to the weight of the evidence – not to its admissibility").[5]

[5] Defendant's motion appears to be premature. Courts have observed that, "[e]vidence may be authenticated in many ways" and "the 'type and quantum' of evidence necessary to authenticate a web page will always depend on context." *United States v. Ulbricht*, 79 F. Supp. 3d 466, 488 (S.D.N.Y. 2015) (quoting *Vayner*, 769 F.3d at 133). Courts also have expressed skepticism that "authentication of evidence derived from the Internet require[s] 'greater scrutiny' than authentication of any other record." *Id.* In this regard, "Whether the Government can meet Rule 901's authentication standard with respect to the challenged exhibits is a question best answered at trial. There simply is no basis to prejudge the Government's ability to meet that standard." *Id.*

This is especially true here. The United States continues to investigate and is working to procure witness testimony not only to authenticate the messages obtained by the FBI (i.e., the messages obtained directly from the dark websites), but also to obtain screenshots of the additional messages obtained by

3. The Messages *Sent to Defendant* are Admissible to Establish the Effect on the Listener and to Put Defendant's Messages in Context.

As set forth above, Defendant's own statements and messages to the dark web hitmen are admissible as statements against an opposing party. *See* Fed. R. Evid. 801(d)(2)(A). In this regard, excerpts of communications Defendant received *in response* to Defendant's solicitations serve the non-hearsay purpose of providing context for Defendant's admissions – including to demonstrate the impact of those messages on Defendant's state of mind. Addressing this issue, the Second Circuit blessed the admission of text message communications with a defendant, even when the author of the communications does not testify:

> Although the authors of the "Project 9" messages did not testify at trial, the messages were not hearsay because they were not offered in evidence to prove the truth of the matters asserted. The prosecution offered the Project 9 messages to provide context for defendants' messages sent in response to them, messages whose admissibility is not contested.

United States v. Dupre, 462 F.3d 131, 137 (2d Cir. 2006); *see also United States v. Whitman*, 771 F.2d 1348, 1352 (9th Cir. 1985) (admitting both sides of a conversation when a non-testifying witness's statements are offered to place defendant's response in context).

Consistent with *Dupre*, courts have explained that messages to a defendant from a non-testifying third-party are relevant when such messages put Defendant's own communications in context: "[T]o the extent the incoming messages are not offered to prove the truth of the matter asserted, but are included to provide context for the outgoing

---

the BBC and forwarded to the FBI. Because of this somewhat evolving evidentiary landscape in the run-up to trial, this Court may decide to reserve judgment on Defendant's motion.

messages attributed to Defendant, they are not hearsay." *United States v. Benford*, 2015 WL 631089, at *4 (W.D. Okla. Feb. 12, 2015), *aff'd*, 875 F.3d 1007 (10th Cir. 2017). The Seventh Circuit has put it like this:

> The hearsay objection is a nonstarter. The text messages Lewisbey sent are his own statements and as such are excluded from the definition of hearsay by Rule 801(d)(2)(A). The messages he received were admitted not for the truth of the matter asserted but instead to provide context for Lewisbey's own messages *See* Fed. R. Evid. 801(c)(2); *United States v. Robinzine*, 80 F.3d 246, 252 (7th Cir. 1996) (Statements offered not to prove "the truth of the matter asserted" but for another legitimate purpose do "not even fit the definition of hearsay.").

Lewisbey, 843 F.3d at 658 (7th Cir. 2016); *see also United States v. Garcia*, 778 F. App'x 779, 785–86 (11th Cir. 2019) ("Any post [Defendant] made or message he sent could be admitted into evidence as a party admission under Federal Rule of Evidence 801(d)(2). Messages [Defendant] received in response could serve the non-hearsay purpose of providing context for the conversation."); *Lamm*, 5 F.4th at 948 ("When out-of-court statements are not offered for their truth, but instead to provide context for certain responses, they are not hearsay.").

At trial, the government anticipates introducing excerpts from Defendant's messages, including, but not limited to, conversations with the operators of the Internet Killers and Sinaloa Cartel websites. These messages between Defendant and dark web sites are relevant to show Defendant's state of mind – including, his intent for the hitmen to kidnap and extort his estranged wife. Again, these messages and conversations are admissible at trial because they serve the serve the non-hearsay purpose of providing context for Defendant's own admissions and the effect on the listener – i.e., the effect on Defendant.

Even Defendant's motion recognizes that the messages *sent* to Defendant are not being offered for their truth. Defendant notes that the administrators of the dark websites – offering purported hitmen services in exchange for Bitcoin – were actually trying to

"scam" Defendant. ECF No. 119 at 20. While Defendant clearly believed these were real hitmen – paying $60,000 for their services, the government is not offering the messages that were sent *to* Defendant for their truth – i.e., that they actually were providing hitman services. Rather, messages and information conveyed to Defendant are being offered to show Defendant's intent in the plot to have his estranged wife kidnapped and a colleague assaulted. *See* Fed. R. Evid. 801(c)(2); *see also United States v. Payne*, 944 F.2d 1458, 1472 (9th Cir. 1991) ("We find that the statement properly was treated as non-hearsay because it was not introduced for the truth of the matter asserted . . . . Rather, it was introduced to show the effect on the listener.").

CONCLUSION

For the foregoing reasons, the United States respectfully submits that Defendant's Motion to Exclude should be denied.

Dated: July 8, 2022

Vanessa R. Waldref
United States Attorney

/s/ Richard R. Barker
Richard R. Barker
Patrick J. Cashman
Assistant United States Attorneys

CERTIFICATE OF SERVICE

I hereby certify that on July 8, 2022, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF System which will send notification of such filing to counsel of record.

/s/ Richard R. Barker
Richard R. Barker
Assistant United States Attorney